

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 152 109 A2

(12)

DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
07.11.2001 Bulletin 2001/45

(51) Int Cl.7: E05B 49/00, B60R 25/00

(21) Numéro de dépôt: 01401096.1

(22) Date de dépôt: 27.04.2001

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(72) Inventeur: Lelandais, Guy
91190 Gif-sur-Yvette (FR)

(30) Priorité: 03.05.2000 FR 0005629

(74) Mandataire: Abello, Michel
Cabinet Peusset,
78, avenue Raymond Poincaré
75116 Paris (FR)

(71) Demandeur: Delphi Technologies, Inc.
Troy, MI 48007 (US)

(54) Système pour le démarrage et/ou l'accès mains libres d'un véhicule automobile

(57) Système d'accès dit mains libres pour véhicule automobile (V), comportant une unité centrale apte à engendrer, à une cadence d'horloge haute prédéterminée un signal numérique représentatif de données d'authentification émis sous la forme d'un signal d'interrogation radio-fréquence, et destiné à être reçu par un dispositif d'identification (I), qui comporte une première boucle à verrouillage de phase (135) pour délivrer un signal d'horloge de référence dont la cadence est synchronisée avec celle du signal d'interrogation précité, le dispositif d'identification étant apte à émettre un signal

crypté de réponse (16) en radio-fréquence vers l'unité centrale, et l'unité centrale comportant une deuxième boucle à verrouillage de phase (70) pour délivrer à une unité de décision de bits un signal d'horloge de référence dont la cadence est synchronisée avec celle du signal crypté de réponse, l'unité centrale comportant, en outre, un moyen pour déterminer le décalage temporel entre ledit signal (V10) délivré par l'unité de décision de bits et un signal crypté correspondant (V11) engendré par l'unité centrale à ladite haute cadence prédéterminée.

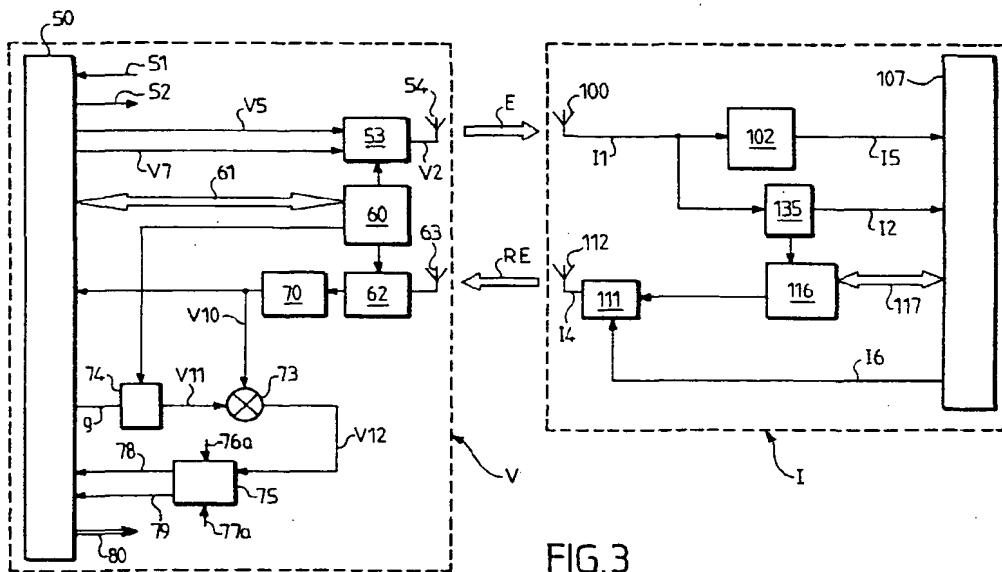


FIG.3

Description

[0001] La présente invention concerne un système d'accès dit mains libres pour véhicule automobile, c'est à dire un système de communication non filaire permettant d'entrer dans le véhicule sans clé. Ce système peut également s'appliquer au démarrage mains libres du véhicule, c'est à dire au démarrage sans clé.

[0002] Un tel système comporte généralement un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique. L'initialisation du protocole de communication peut être activée en actionnant la poignée extérieure de porte, pour l'accès mains libres, ou en appuyant sur un bouton de démarrage, dans le mode démarrage mains libres. Le système est apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite pré-déterminée du véhicule, généralement de l'ordre de quelques mètres, pour éviter, d'une part les interférences avec d'autres sources de signaux de l'environnement, et, d'autre part, pour éviter le fonctionnement du système à une distance telle que l'utilisateur est trop éloigné du véhicule pour être conscient des opérations effectuées par ledit système.

[0003] Certains systèmes actuellement proposés utilisent des systèmes à induction magnétique à très courte portée, pour à la fois alimenter en énergie et transporter les informations depuis l'unité centrale du véhicule vers le dispositif d'identification qui se trouve dans le champ électromagnétique engendré par les antennes du véhicule. Toutefois, un tel système ne permet une communication qu'à très courte distance du véhicule de l'ordre de quelques cm. Un autre système couramment proposé consiste à utiliser des ondes porteuses à basse fréquence, de l'ordre de 125 kHz pour la communication depuis le véhicule vers le dispositif d'identification, et des ondes porteuses à ultra haute fréquence, par exemple de l'ordre de 434 ou 868 MHz, pour la zone Europe, et de 315 ou 902 MHz pour la zone USA. Toutefois, dans ce cas, le dispositif d'identification doit comporter une pile pour alimenter ses circuits électroniques propres. Pour minimiser la consommation électrique, on peut prévoir, à titre d'exemple, que le dispositif d'identification soit en sommeil pendant 9 ms et en éveil 1 ms, pendant des périodes de 10 ms.

[0004] Bien entendu, la communication bidirectionnelle entre le véhicule et le dispositif d'identification est cryptée, afin d'éviter tout fonctionnement intempestif du système et pour le sécuriser vis à vis des malfaiteurs. Sur la figure 1 des dessins annexés, on a représenté un exemple de système d'encryptage déjà connu. Sur cette figure 1, on a représenté un véhicule V qui comporte

dans son unité centrale une mémoire 1 contenant une clé secrète K et un générateur de nombres aléatoires 2, les nombres aléatoires R engendrés ayant, par exemple, une longueur de 56 bits. Ce nombre aléatoire R est émis vers le dispositif d'identification I, comme indiqué par la flèche 3. Simultanément, ce même nombre aléatoire R est mélangé avec la clé secrète K suivant une fonction associative complexe f, dans un mélangeur 4 qui est relié à son entrée à la mémoire 1 et au générateur de nombres aléatoires 2. Le mélangeur 4 délivre, en sortie, un signal représentatif du mélange de la clé secrète K et du nombre aléatoire R, à savoir le signal f(R, K). Ce signal est mémorisé dans une mémoire 5 reliée à la sortie du mélangeur 4. Ce signal est envoyé au dispositif d'identification I, sous la forme d'un signal d'une longueur par exemple de 28 bits, comme indiqué par la flèche 6. Dans le véhicule V, le signal f(R, K) est mélangé à nouveau à la clé secrète K dans un mélangeur 7, qui est relié à son entrée aux mémoires 1 et 5 précitées. Ce mélangeur 7 mélange les deux signaux suivant une fonction associative complexe g. Le véhicule V mémorise alors dans une mémoire 8 reliée à la sortie du mélangeur 7 le signal représentatif du mélange, à savoir le signal g(R, f, K).

[0005] Du côté du dispositif d'identification, la même clé secrète K est mémorisée dans une mémoire 11 et un mélangeur 14 ayant la même fonction associative f reçoit en entrée la clé secrète fournie par la mémoire 11 du dispositif d'identification I et le nombre aléatoire R reçu par le dispositif d'identification en provenance du véhicule. Le dispositif d'identification I mémorise le signal en sortie du mélangeur 14 dans une mémoire 15 et compare ce signal dans un comparateur 16 avec le signal reçu suivant la flèche 6 en provenance du véhicule V. Si les deux signaux ne sont pas identiques, sous réserve du temps de retard propre au matériel et à la transmission du signal dans la zone de transmission autorisée, le dispositif d'identification interrompt la communication comme étant non-autorisée. En revanche, si les deux signaux correspondent, le signal est mélangé dans un mélangeur 17 avec la clé secrète fournie par la mémoire 11 du dispositif d'identification I, suivant la même fonction associative g précitée. Le signal de sortie du mélangeur 17 est mémorisé dans une mémoire 18 du dispositif d'identification pour être ensuite envoyé vers le véhicule suivant la flèche 9 sous la forme d'un signal ayant une longueur par exemple de 20 bits. Enfin, le signal reçu par la flèche 9 est comparé avec le signal reçu de la mémoire 8 du véhicule dans un comparateur 10. Si ces deux signaux correspondent, sous réserve des retards dus au temps de réponse du matériel et de la transmission du signal dans la zone autorisée, le reste de la communication est autorisé et l'unité centrale du véhicule pourra, le cas échéant, commander la condamnation ou la décondamnation des serrures des ouvrants du véhicule. Bien entendu, un autre protocole de cryptage pourra être utilisé pour sécuriser la transmission des données.

[0006] Toutefois, malgré ce protocole de cryptage, il existe une façon de pirater le système, sans connaître ni la clé secrète, ni les différentes fonctions associatives du protocole d'encryptage. Ce procédé de piratage est représenté sur la figure 2. Selon ce procédé, on suppose que l'utilisateur U qui porte le dispositif d'identification I est situé à une distance du véhicule V supérieure à la distance autorisée de communication, par exemple de 10 à 100 m de distance du véhicule. Dans ce cas, un pirate équipé d'un premier boîtier relais 20 peut s'approcher du véhicule V à une distance suffisante pour communiquer avec celui-ci, par exemple à une distance de l'ordre de 1 à 5 m. Ce pirate actionne le début de la communication, par exemple en tirant sur la poignée extérieure de portière. Ceci déclenche l'émission des signaux basse fréquence par le véhicule vers le boîtier relais 20, comme indiqué par la flèche en zig-zag 21. Ce signal 21 envoyé par le véhicule est reçu par une bobine 22 du boîtier relais 20, qui est reliée à un récepteur 23 à 125 kHz. Ce récepteur 23 est relié à un émetteur à large bande à haute fréquence, de l'ordre de plusieurs MHz. L'émetteur 24 émet via son antenne 25, comme représenté par la flèche 26, vers un deuxième boîtier relais 30, qui est porté par un autre pirate qui suit de près l'utilisateur U. L'échange d'informations entre les deux boîtiers relais 20 et 30 s'effectuant à très haute fréquence, il est possible d'effectuer cette communication à grande distance. Le deuxième boîtier relais 30 comporte une antenne 31 pour recevoir le signal 26 émis par le boîtier relais 20. L'antenne 31 est reliée à un récepteur large bande à la même fréquence que l'émetteur 24 du premier boîtier relais 20. Le signal ainsi reçu est retransmis à basse fréquence à 125 kHz par un émetteur 33 qui est relié à une bobine d'émission 34 afin d'envoyer un signal 35 vers le dispositif d'identification I qui soit conforme au signal 21 émis par le véhicule. Le signal 35 étant la répétition du signal authentique du véhicule, le dispositif d'identification I va le reconnaître et émettre à son tour son signal de réponse 36, ledit signal de réponse 36 étant envoyé à haute fréquence et reçu par une antenne 37 du deuxième boîtier relais 30, par exemple à 434 MHz. L'antenne 37 est reliée à un récepteur 38, qui va convertir le signal à 434 MHz en un signal à une fréquence différente, par exemple à 315 MHz. Le signal est alors émis par un émetteur à large bande 39 via une antenne 40 vers le premier boîtier relais 20, cette différence de fréquence étant nécessaire pour que les différents signaux n'interfèrent pas entre eux. Bien entendu, la fréquence du signal 41 émis en retour par le deuxième boîtier relais 30 est différente à la fois de la fréquence du signal 26 et du signal 36. Ce signal 41 est capté par une antenne 27 du premier boîtier relais 20, ladite antenne 27 étant reliée à un récepteur large bande 28 de la même fréquence que l'émetteur 39. Le récepteur 28 est relié à un émetteur 29 qui transforme le signal à 315 MHz en un signal à 434 MHz qui est envoyé via l'antenne 42 du premier boîtier relais 20 vers le véhicule V, comme représenté par la flèche

en zig-zag 43.

- [0007]** Il suffit que les pirates utilisent des boîtiers relais ayant des liaisons à large bande, par exemple supérieure à 50 MHz, ce qui est possible car les systèmes pirates n'ont pas à respecter les réglementations ; le temps de transit supplémentaire dû à la distance peut être alors de l'ordre de quelques nanosecondes, ce qui est négligeable en comparaison avec les constantes de temps nécessaires pour la transmission normale autorisée. A titre d'exemple, la communication totale peut être de l'ordre de 20 à 40 ms, et la durée totale du fonctionnement du système pour déclencher la décondamnation ou la condamnation des serrures électriques peut être de l'ordre de 100 ms.
- [0008]** Pour détecter un tel piratage et interrompre la communication, une solution pourrait consister à mesurer le temps de propagation des ondes radio UHF, en comparant ce temps mesuré avec un temps prédéterminé correspondant à une communication dans une zone limitée autorisée autour du véhicule. Ce temps de propagation, compte tenu des distances concernées, est très faible, de l'ordre de quelques ns à quelques dizaines de ns. Pour différencier des temps aussi courts, on a habituellement recours à des bandes passantes très larges de l'ordre de 10 MHz. L'intérêt de la présente invention consiste à avoir recours à une bande passante, nettement moins large, par exemple de l'ordre de 1 MHz, telle que par exemple à la fréquence de 433,9 MHz.
- [0009]** L'invention a pour but d'éliminer les inconvénients précités et de proposer un système d'accès dit mains libres pour véhicule automobile, permettant de détecter un piratage du système, notamment par l'intermédiaire de boîtiers relais, en prenant compte du temps de propagation du signal entre le véhicule et le dispositif d'identification.
- [0010]** A cet effet, l'invention a pour objet un système d'accès dit mains libres pour véhicule automobile, comportant un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite pré-déterminée du véhicule, caractérisé par le fait que ladite unité centrale est apte à engendrer, à une cadence d'horloge haute prédéterminée, lors de la communication, un signal numérique représentatif de données d'authentification, ledit signal étant apte à être émis sous la forme d'un signal d'interrogation radio-fréquence par l'unité centrale, et destiné à être reçu par le dispositif d'identification, qui comporte une première boucle à verrouillage de phase pour délivrer un signal d'horloge de référence dont la cadence est synchronisée

avec celle du signal d'interrogation précité, le dispositif d'identification étant apte à émettre un signal crypté de réponse en radio-fréquence vers l'unité centrale à ladite cadence de référence, et l'unité centrale comportant une deuxième boucle à verrouillage de phase pour délivrer à une unité de décision de bits un signal d'horloge de référence dont la cadence est synchronisée avec celle du signal crypté de réponse, ladite unité de décision de bits étant apte à recevoir ledit signal crypté de réponse en provenance du dispositif d'identification, pour délivrer à ladite cadence de référence, un signal numérique représentatif dudit signal crypté de réponse, l'unité centrale comportant, en outre, un moyen pour déterminer le décalage temporel entre ledit signal délivré par l'unité de décision de bits et un signal crypté correspondant engendré par l'unité centrale à ladite haute cadence pré-déterminée, l'unité centrale étant apte à détecter une tentative de piratage provoquant l'arrêt de ladite communication, lorsque ledit décalage temporel déterminé est supérieur à une première valeur de seuil pré-déterminée.

[0011] Avantageusement, ledit moyen de détermination de l'unité centrale comporte un mélangeur apte à mélanger, d'une part, le signal délivré en sortie de l'unité de décision de bits à ladite cadence de référence et, d'autre part, ledit signal crypté correspondant engendré par l'unité centrale à ladite cadence pré-déterminée pour délivrer en sortie du mélangeur un signal représentatif des décalages temporels successifs de chaque bit dudit signal crypté de réponse, le mélangeur étant relié à un intégrateur pour faire la somme des temps de réponse liés à chaque créneau de décalage temporel de bit dudit signal, la sortie dudit intégrateur étant reliée à au moins un premier comparateur pour comparer ladite somme de temps de réponse avec ladite première valeur de seuil pré-déterminée. Dans ce cas, on peut prévoir que la somme des temps de réponse effectuée par l'intégrateur est arrêtée lorsque l'unité centrale de commande détecte la réception du dernier bit du signal crypté de réponse en provenance du dispositif d'identification.

[0012] Selon une autre caractéristique, la sortie de l'intégrateur est reliée à au moins un second comparateur pour comparer ladite somme de temps de réponse avec une autre valeur de seuil pré-déterminée inférieure à ladite première valeur de seuil pré-déterminée, au-delà de laquelle est détectée une communication au-delà de la distance limite pré-déterminée.

[0013] Selon encore une autre caractéristique, le dispositif d'identification comporte un détecteur de fin de trame du signal d'interrogation, apte à déclencher l'émission du signal crypté de réponse, à ladite cadence de référence par le dispositif d'identification, lorsque la fin de la trame du signal d'interrogation est détectée. Dans ce cas, on peut prévoir que ledit détecteur de fin de trame est apte à reconnaître soit des données de fin d'interrogation dans ledit signal d'interrogation, soit des données de début d'interrogation dans ledit signal d'interrogation, pour en déduire la fin de sa trame en fonc-

tion du nombre pré-déterminé de bits devant être reçus par le dispositif d'identification en provenance de l'unité centrale.

[0014] On peut prévoir que le dispositif d'identification 5 comporte un oscillateur générateur d'onde porteuse en radio-fréquence, relié en sortie à un modulateur de phase ou d'amplitude, qui est commandé par le signal numérique crypté de réponse du dispositif d'identification. Le dispositif d'identification peut également comporter 10 une unité de décision de bits dont la cadence de référence est délivrée par la première boucle de verrouillage de phase, ladite unité de décision de bits recevant en entrée le signal d'interrogation, pour délivrer en sortie un signal numérique à ladite cadence de référence, représentant ledit signal d'interrogation, par exemple en vue de comparer ledit signal avec un signal correspondant engendré par le dispositif d'identification.

[0015] Avantageusement, le signal délivré en sortie 15 par l'unité de décision de bits de l'unité centrale est comparé par cette dernière avec un signal numérique crypté correspondant engendré par l'unité centrale, afin d'authentifier le dispositif d'identification.

[0016] On peut également prévoir que l'unité centrale 20 comporte un oscillateur générateur d'onde porteuse en radio-fréquence, relié à un modulateur de phase ou d'amplitude, qui est commandé par ledit signal numérique d'interrogation engendré par l'unité centrale.

[0017] Dans une forme de réalisation particulière, l'unité centrale est apte à commander successivement 25 l'arrêt puis le démarrage de l'oscillateur de l'unité centrale, selon que celle-ci est en phase d'émission du signal d'interrogation, puis en phase de réception du signal de réponse.

[0018] L'invention sera mieux comprise, et d'autres 30 buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description explicative détaillée qui va suivre d'un mode de réalisation particulier de l'invention, donné uniquement à titre illustratif et non limitatif, en référence au dessin schématique annexé, dans lequel :

- la figure 1 est un schéma synoptique fonctionnel représentant le protocole d'encryptage pour sécuriser la transmission bidirectionnelle de données entre un véhicule et un dispositif d'identification ;
- la figure 2 est un schéma synoptique fonctionnel illustrant un moyen de piratage du système d'encryptage par l'intermédiaire de deux boîtiers relais ;
- la figure 3 est un schéma synoptique fonctionnel simplifié d'un système d'accès mains libres conforme à l'invention ;
- la figure 4 est un schéma synoptique fonctionnel plus détaillé correspondant au schéma de la figure 3 ;
- la figure 4A est un schéma synoptique fonctionnel d'un détail du dispositif d'identification représenté sur la figure 4 ;
- la figure 5 représente plusieurs chronogrammes il-

lustrant les trames complètes d'interrogation émises et reçues par le véhicule et par le dispositif d'identification ;

- la figure 6 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 5, indiquée par la flèche VI, au cours de la séquence d'interrogation par le véhicule ; et
- la figure 7 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 5, indiquée par la flèche VII, au cours de la séquence de réponse par le dispositif d'identification.

[0019] On va maintenant se référer aux figures 3 et 4, qui représentent le système d'accès mains libres selon l'invention respectivement sous forme simplifiée et plus détaillée.

[0020] Le véhicule automobile V comporte dans son unité centrale un micro-contrôleur 50, qui est généralement dans un état de semi-sommeil ou d'attente d'un réveil. Lorsque l'utilisateur actionne la poignée extérieure de porte, un signal d'activation est envoyé au micro-contrôleur 50, comme indiqué par la flèche 51. En réponse, le micro-contrôleur envoie un signal d'alimentation général, comme représenté par la flèche 52, pour alimenter les différents composants électroniques de l'unité centrale. Puis, le micro-contrôleur 50 engendre un signal d'éveil e à faible cadence sk, par exemple de l'ordre de 2 à 100 Kb/s sur la ligne V5. La ligne V5 est reliée à un émetteur 53 pour émettre via une antenne 54 les signaux vers le dispositif d'identification I comme représenté par la flèche E. L'émetteur 53 comporte, comme mieux visible sur la figure 4, un oscillateur 55 pour engendrer une onde porteuse à haute fréquence, par exemple à quelques centaines de MHz, ledit oscillateur étant alimenté par la ligne 52. L'oscillateur 55 est relié à un modulateur de phase 56 ou un modulateur d'amplitude du type à modulation à 50 % et à 100 % selon que la valeur du bit transmis est à 0 ou 1, dont la sortie est reliée à l'antenne 54 précitée.

[0021] Le signal émis E, par exemple avec une amplitude de l'ordre de 2V efficace, est reçu par une antenne 100 du dispositif d'identification I avec une atténuation de l'ordre de -40 dBm, ce qui représente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le dispositif d'identification présente une amplitude de l'ordre de 20 mV. L'antenne 100 est reliée, via la ligne I1, à un filtre radio-fréquence 101 (uniquement représenté sur la figure 4) pour éliminer les fréquences parasites. La sortie du filtre 101 est reliée à un embranchement, d'une part, vers un récepteur à faible cadence et à faible consommation 102 et, d'autre, part à un amplificateur logarithmique 103 qui permet de délivrer en sortie un signal de l'ordre de 2V efficace, et sort de récepteur haute fréquence. Les signaux à faible cadence sk ne sont pas transmis par l'amplificateur 103, mais passent essentiellement via le récepteur 102. Comme mieux visible sur la figure 4, le récepteur 102 comprend successivement un détecteur d'enveloppe

radio-fréquence 104 pour reconstituer les signaux à faible cadence sur la ligne 15, qui correspondent à ceux de la ligne V5. La sortie du détecteur d'enveloppe 104 est reliée à un amplificateur basse fréquence 105, dont la sortie est reliée à un décodeur de séquence d'éveil 106. Au démarrage de la communication avec le véhicule, seul le décodeur 106 est alimenté en permanence par la pile du dispositif d'identification. Autrement dit, les données d'éveil e sont décodées par le décodeur 106, afin d'envoyer un ordre d'éveil au micro-contrôleur 107, à la sortie du décodeur 106. Le micro-contrôleur 107 éveille alors tous les autres composants électroniques du dispositif d'identification. Ainsi, les données suivantes, à savoir les signaux R, f et s, sont transmis au micro-contrôleur 107 via l'amplificateur 103.

[0022] Après émission des données d'éveil e, le micro-contrôleur 50 du véhicule V engendre, à la cadence lente sk du micro-processeur, un signal numérique représentatif d'un nombre aléatoire R d'une longueur, par exemple de 56 bits, un signal numérique représentatif de la fonction f(R, K) d'une longueur par exemple de 28 bits, et un signal représentatif de données de service s, par exemple d'une longueur de 100 à 5 000 bits, par exemple des données sur la maintenance, le réglage du véhicule, etc (voir figure 5), lesdits signaux R, f, s étant reçus par une mémoire-tampon 58, pour délivrer en sortie lesdits signaux à haute cadence fk, sur une ligne V7. La sortie de la mémoire tampon 58 est reliée au modulateur de phase ou d'amplitude 56 pour moduler en phase l'onde porteuse engendrée par l'oscillateur 55, chaque signal étant transmis sous la forme d'un signal radio-fréquence via l'antenne 54 en direction du dispositif d'identification I. La trame globale d'émission V2 des signaux par l'antenne 54 est illustrée sur la figure 5. En se référant plus particulièrement à la figure 6, on a représenté, à plus grande échelle, une portion de la trame d'interrogation sur la ligne V2. Chaque bit d'interrogation est porté par une onde oscillante à haute fréquence ayant un temps bit par exemple de l'ordre de 500 ns pour une cadence fk de l'ordre de 2 Mb/s. Bien entendu, la fréquence fk pourrait être plus faible, ce qui entraînerait un temps bit d'autant plus long. Une unité de gestion de base de temps 60 du véhicule V est apte à délivrer les signaux d'horloge à faible cadence sk et à haute cadence fk sur la base d'un signal délivré par un quartz 69. Bien entendu, l'unité 60 est reliée au micro-contrôleur 50, comme indiqué par la double flèche 61. L'unité 60 commande successivement l'arrêt ou le démarrage de l'oscillateur 55 de l'émetteur 53 et d'un amplificateur 65 d'un récepteur 62 de l'unité centrale.

[0023] Le dispositif d'identification I reçoit via son antenne 100 sur la ligne I1 un signal qui correspond au signal d'interrogation émis par le véhicule V, avec un temps retard δ qui correspond au temps de propagation du signal entre le véhicule et le dispositif d'identification. Le signal passe alors par l'amplificateur 103, ce dernier délivrant en sortie un signal représenté sur la ligne I12 à la figure 6, qui correspond à l'enveloppe du signal ana-

logique reçu par le dispositif d'identification en provenance du véhicule. On constate sur la figure 6 que le signal I12 en sortie de l'amplificateur 103 présente une forme générale en créneaux, dont les fronts O descendants et montants sont inclinés et peuvent varier sur une certaine plage de valeur, compte tenu des déformations du signal à travers les filtres d'émission du véhicule et de réception du dispositif d'identification. Ces légères variations sur le signal I12 sont symbolisées par des traits triples sur les fronts O montants et descendants des créneaux du signal I12. Pour redresser ce signal I12, la sortie de l'amplificateur 103 est reliée à une unité de remise en forme 108 qui délivre en sortie un signal carré I2 en fonction du passage à 0V du signal analogique I12 en sortie de l'amplificateur 103. L'unité de remise en forme 108 est reliée à une unité de synchronisation de bits à boucle de verrouillage de phase 135. Comme mieux visible sur la figure 4, cette unité 135 comporte, à partir de la sortie de l'unité de remise en forme 108, un embranchement entre, d'une part, une boucle à verrouillage de phase 109 et, d'autre part, une unité de décision de bits 115. Comme mieux visible sur la figure 4A, la boucle à verrouillage de phase 109 comporte un mélangeur 130 recevant, d'une part, le signal en sortie de l'unité de remise en forme 108 et, d'autre part, un signal provenant d'un oscillateur 132 commandé en tension. Le mélangeur 130 délivre en sortie un signal d'erreur qui est reçu par un filtre de boucle constitué d'un filtre passe-bas du premier ordre 131 qui délivre une tension d'erreur pour commander l'oscillateur 132, afin d'accélérer ou de retarder les oscillations, en cas de retard ou d'avance du signal en sortie de l'oscillateur 132 par rapport au signal délivré par l'unité de remise en forme 108 afin de synchroniser les signaux. La sortie de l'oscillateur 132 est également reliée à l'unité de décision de bits 115, pour lui fournir la phase de référence précise du signal d'émission du véhicule. Ainsi, l'unité de décision de bits 115 peut délivrer en sortie un signal analogique représentatif des bits du signal d'interrogation reçu en provenance du véhicule, selon la cadence de référence f'k délivrée par la boucle à verrouillage de phase 109 qui a permis de synchroniser ladite cadence avec celle f'k du véhicule. La sortie de l'unité de décision de bits 115 est reliée à un embranchement entre, d'une part, un détecteur de fin de trame 119 et, d'autre part, une mémoire-tampon 118 recevant le signal en sortie de l'unité de décision de bits 115 à la cadence élevée de référence f'k, pour le restituer à la cadence lente sk au micro-contrôleur 107 du dispositif d'identification I, afin que ce dernier puisse authentifier le signal d'interrogation, par exemple comme indiqué à l'étape 16 de la figure 1. En variante, la boucle à verrouillage de phase analogique 109 pourrait être réalisée de façon numérique, en utilisant un diviseur très rapide à 100 MHz ou plus, piloté par un quartz, et associé à une logique de comptage.

[0024] Le détecteur de fin de trame 119 est apte à reconnaître des données de fin d'interrogation dans ledit

signal d'interrogation, afin de déclencher ultérieurement l'émission du signal de réponse par le dispositif d'identification. En variante, le détecteur 119 est apte à reconnaître des données de début d'interrogation dans ledit signal d'interrogation, et à en déduire la fin de la réception dudit signal par le dispositif d'identification en connaissant le nombre prédéterminé de bits d'interrogation devant être reçus par le dispositif d'interrogation en provenance du véhicule V. Ainsi, il n'est pas possible qu'un pirate piége le détecteur 119 en écourtant l'émission du signal par le véhicule V, car ce détecteur 119 attendra soit les bits de fin d'interrogation soit le nombre de bits pré-déterminé à compter du début de l'interrogation. Fonctionnellement, le détecteur 119 fait partie d'une unité de gestion de base de temps 116 qui est reliée au micro-contrôleur 107 via la ligne 117 et qui délivre les signaux d'horloge sk et f'k. La cadence d'horloge de référence f'k est fournie par la boucle à verrouillage de phase 109 au détecteur 119, comme représenté par une flèche. La mémoire-tampon 118 est apte à envoyer les signaux R, f et s au micro-contrôleur 107 du dispositif d'identification. Dans le dispositif d'identification, le signal d'horloge de référence f'k est délivré par la boucle à verrouillage de phase 109 et non par un quartz, contrairement au véhicule V.

[0025] A la fin de la réception du signal d'interrogation par le dispositif d'identification, le détecteur de fin de trame 119 est apte à déclencher, d'une part, le démarrage d'un oscillateur générateur d'ondes porteuses en radiofréquence 113, qui fait partie d'un émetteur 111 du dispositif d'identification et, d'autre part, le fonctionnement d'une mémoire-tampon 110 qui reçoit du micro-contrôleur 107 le signal g à la faible cadence sk, afin de délivrer en sortie ledit signal g à la haute cadence de référence f'k, comme représenté sur la ligne 16 visible sur la figure 7. A la suite du signal crypté de réponse g, des données de service s peuvent également être transmises par le dispositif d'identification vers le véhicule V, comme indiqué sur la figure 5. Le signal crypté de réponse g vient commander un modulateur de phase ou d'amplitude 114 qui fait partie de l'émetteur 111, ledit modulateur 114 recevant en entrée l'onde porteuse délivrée par l'oscillateur 113 et étant relié en sortie à une antenne 112 pour l'émission du signal de réponse RE vers le véhicule V.

[0026] En partant de l'hypothèse que les signaux électromagnétiques transmis se propagent à la vitesse de la lumière, à savoir $3 \cdot 10^8$ m/s, on peut considérer que la durée de transmission des signaux est de l'ordre de 3 ns par mètre de distance entre le véhicule et le dispositif d'identification I. Autrement dit, pour un trajet aller-retour entre le véhicule V et le dispositif d'identification I, espacé d'une distance d'environ 5 mètres, la

durée de propagation δ serait de l'ordre de 30 ns. A cette durée de propagation δ , on pourrait ajouter le temps de réponse des circuits électroniques, qui pourrait être de l'ordre de quelques ns ou dizaines de ns, selon la bande passante attribuée à la porteuse.

[0027] Le signal de réponse RE émis par le dispositif d'identification I est reçu par un récepteur 62 via une antenne 63, avec une atténuation de l'ordre de -40 dBm, ce qui représente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le véhicule présente une amplitude de l'ordre de 20 mV. Comme mieux représenté sur la figure 4, le récepteur 62 comporte un filtre radio-fréquence 64 relié à l'antenne 63, dont le signal de sortie est délivré à l'entrée de l'amplificateur logarithmique 65 qui présente un gain de 80 dB, ce qui permet d'atteindre un coefficient de multiplication allant jusqu'à 10 000 fois, et notamment de délivrer en sortie dudit amplificateur 65 un signal de l'ordre de 2V efficace. L'amplificateur 65 est commandé par l'unité 60 et est relié en sortie à un circuit de remise en forme 66, analogue à l'unité 108 du dispositif d'identification.

[0028] La sortie du circuit de remise en forme 66 est reliée à une unité de synchronisation de bits à boucle à verrouillage de phase 70 analogue à l'unité 135 du dispositif d'identification I. Comme mieux visible sur la figure 4, la sortie du circuit de remise en forme 66 est reliée à un embranchement entre, d'une part, une unité de décision de bits 67 et, d'autre part, une boucle à verrouillage de phase 68 qui délivre en sortie un signal V8 représentatif de la cadence d'horloge de référence rk, vers l'unité de décision de bits 67. La structure de la boucle à verrouillage de phase 68 est analogue à celle de la boucle 109 du dispositif d'identification I. L'unité de décision de bits 67 délivre en sortie un signal V10 qui est représentatif du signal crypté de réponse g émis par le dispositif d'identification I. Comme visible sur la figure 7, le signal V8 est décalé du signal 16 du temps de propagation du signal δ . La sortie de l'unité de décision de bits 67 est reliée à un embranchement entre, d'une part, une mémoire-tampon 72 qui est apte à recevoir à la cadence rk le signal V10 pour le délivrer à la faible cadence sk au micro-contrôleur 50, afin qu'il authentifie le signal de réponse g, comme indiqué par exemple à l'étape 10 de la figure 1 et, d'autre part, une entrée d'une porte logique OU exclusif 73. Pour l'authentification du signal de réponse g reçu en provenance du dispositif d'identification, l'unité centrale du véhicule engendre un signal crypté correspondant g, comme indiqué à l'étape 8 de la figure 1. Il est à noter que cette comparaison entre les deux fonctions g s'effectue par auto-corrélation entre les signaux, le seuil d'auto-corrélation acceptable étant par exemple fixé à 90 %, sachant qu'un niveau d'auto-corrélation de 50 % correspond à la comparaison de deux signaux aléatoires.

[0029] Le micro-contrôleur 50 délivre le signal g propre au véhicule à une mémoire tampon 74 à la cadence sk, afin qu'il la renvoie à la cadence fk à l'autre entrée de la porte logique 73 précitée. On a représenté sur la

ligne V11 le signal g qui correspond exactement au signal g engendré par le dispositif d'identification et émis sur la ligne 16, comme représenté sur la figure 8, mais avec un décalage temporel de 2δ . La porte logique 73 mélange les signaux V10 et V11 afin de ne délivrer en sortie que les décalages dus au temps de propagation du signal entre le véhicule V et le dispositif d'identification I, comme représenté sur la ligne V12. La sortie de la porte logique 73 est reliée à l'entrée d'un intégrateur 75, qui va délivrer en sortie un signal V13 qui va monter par escalier en fonction du temps, pour chaque créneau C représentatif du temps de propagation du signal. La ligne V13 est reliée à un embranchement entre, d'une part, un premier comparateur 76 recevant sur une autre entrée une valeur limite de seuil 76a qui correspond à la distance de piratage, par exemple 5 à 10 mètres et, d'autre part, un second comparateur 77 recevant sur une autre entrée une autre valeur limite de seuil 77a inférieure à la valeur 76a et qui correspond à la distance de communication autorisée, par exemple 1 à 2 mètres. Selon que l'amplitude du signal de sortie sur la ligne V13 est supérieure ou non à cette valeur limite 76a, un signal de tentative de piratage sera envoyé ou non via la ligne 78 par le premier comparateur 76 au micro-contrôleur 50. De manière analogue, si l'amplitude du signal de sortie sur la ligne V13 est supérieure à la valeur 77a, mais inférieure à la valeur 76a, le second comparateur 77 enverra au micro-contrôleur 50 via la ligne 79, un signal indiquant que la communication se fait hors de la distance autorisée, sans toutefois constituer une tentative de piratage. L'intégrateur 75 va effectuer la somme des décalages temporels élémentaires jusqu'à la fin de la trame d'antipiratage, comme indiqué par la flèche 75a, à moins que la communication soit interrompue préalablement par les premier et deuxième comparateurs 76 et 77 précités. Le fait de faire la somme des décalages temporels sur la ligne V13 permet de s'affranchir des contraintes de résolution et des incertitudes de mesure liées à un temps de propagation aussi faible que 50 ns qui peut représenter 10 % d'un temps bit de 500 ns.

[0030] Enfin, le micro-contrôleur 50 peut délivrer différents signaux de sortie aux autres composants du véhicule par la voie 80 représentée sur les figures 3 et 4.

[0031] En variante, on pourrait remplacer les antennes 54 et 63 du véhicule V par une antenne unique 82 représentée en traits interrompus sur la figure 4, laquelle antenne 82 serait reliée à un diplexeur 81 représenté en traits interrompus sur la figure 4, afin de commuter entre le mode de réception et le mode d'émission selon le cas. De manière analogue, on pourrait remplacer les antennes 100 et 112 du dispositif d'identification par une antenne unique 121 reliée à un diplexeur 120, représentés en traits interrompus sur la figure 4. Les diplexeurs 81 et 120 pourraient ainsi communiquer entre eux, comme indiqué par la double flèche T.

[0032] Bien que l'invention ait été décrite en liaison avec un exemple particulier de réalisation, il est bien évi-

dent qu'elle n'y est nullement limitée et qu'elle comprend tous les équivalents techniques des moyens décrits ainsi que leurs combinaisons si celles-ci entrent dans le cadre de l'invention.

5

Revendications

1. Système d'accès dit mains libres pour véhicule automobile (V), comportant un dispositif d'identification (I) destiné à être porté par un utilisateur (U) et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, **caractérisé par le fait que** ladite unité centrale est apte à engendrer, à une cadence d'horloge haute prédéterminée (f_k), lors de la communication, un signal numérique (V7) représentatif de données d'authentification, ledit signal étant apte à être émis sous la forme d'un signal d'interrogation radio-fréquence (V2) par l'unité centrale, et destiné à être reçu par le dispositif d'identification (I), qui comporte une première boucle à verrouillage de phase (109) pour délivrer un signal d'horloge de référence (f_k) dont la cadence est synchronisée avec celle (f_k) du signal d'interrogation précité, le dispositif d'identification étant apte à émettre un signal crypté de réponse (g) en radio-fréquence vers l'unité centrale à ladite cadence de référence, et l'unité centrale comportant une deuxième boucle à verrouillage de phase (68) pour délivrer à une unité de décision de bits (67) un signal d'horloge de référence (r_k) dont la cadence est synchronisée avec celle du signal crypté de réponse, ladite unité de décision de bits étant apte à recevoir ledit signal crypté de réponse en provenance du dispositif d'identification, pour délivrer, à ladite cadence de référence, un signal numérique (V10) représentatif dudit signal crypté de réponse, l'unité centrale comportant, en outre, un moyen pour déterminer le décalage temporel entre ledit signal (V10) délivré par l'unité de décision de bits (67) et un signal crypté correspondant (V11) engendré par l'unité centrale à ladite haute cadence prédéterminée (f_k), l'unité centrale étant apte à détecter une tentative de piratage provoquant l'arrêt de ladite communication, lorsque ledit décalage temporel déterminé est supérieur à une première valeur de seuil prédéterminée (76a).

2. Système selon la revendication 1, **caractérisé par le fait que** ledit moyen de détermination de l'unité

centrale comporte un mélangeur (73) apte à mélanger, d'une part, le signal (V10) délivré en sortie de l'unité de décision de bits (67) à ladite cadence de référence (r_k) et, d'autre part, ledit signal crypté correspondant (V11) engendré par l'unité centrale à ladite cadence prédéterminée (f_k) pour délivrer en sortie du mélangeur un signal (V12) représentatif des décalages temporels successifs de chaque bit dudit signal crypté de réponse (g), le mélangeur étant relié à un intégrateur (75) pour faire la somme des temps de réponse liés à chaque créneau (C) de décalage temporel de bit dudit signal (V12), la sortie dudit intégrateur étant reliée à au moins un premier comparateur (76) pour comparer ladite somme de temps de réponse avec ladite première valeur de seuil prédéterminée (76a).

3. Système selon la revendication 2, **caractérisé par le fait que** la somme des temps de réponse effectuée par l'intégrateur (75) est arrêtée lorsque l'unité centrale de commande détecte la réception (75a) du dernier bit du signal crypté de réponse en provenance du dispositif d'identification (I).
4. Système selon la revendication 2 ou 3, **caractérisé par le fait que** la sortie de l'intégrateur (75) est reliée à au moins un second comparateur (77) pour comparer ladite somme de temps de réponse avec une autre valeur de seuil prédéterminée (77a) inférieure à ladite première valeur de seuil prédéterminée (76a), au-delà de laquelle est détectée une communication au-delà de la distance limite prédéterminée.
5. Système selon l'une des revendications 1 à 4, **caractérisé par le fait que** le dispositif d'identification (I) comporte un détecteur de fin de trame (119) du signal d'interrogation, apte à déclencher l'émission du signal crypté de réponse (16), à ladite cadence de référence (f_k) par le dispositif d'identification, lorsque la fin de la trame du signal d'interrogation est détectée.
6. Système selon la revendication 5, **caractérisé par le fait que** ledit détecteur de fin de trame (119) est apte à reconnaître soit des données de fin d'interrogation dans ledit signal d'interrogation, soit des données de début d'interrogation dans ledit signal d'interrogation, pour en déduire la fin de sa trame en fonction du nombre prédéterminé de bits devant être reçus par le dispositif d'identification (I) en provenance de l'unité centrale.
7. Système selon l'une des revendications 1 à 6, **caractérisé par le fait que** le dispositif d'identification (I) comporte un oscillateur (113) générateur d'onde porteuse en radio-fréquence, relié en sortie à un modulateur de phase ou d'amplitude (114), qui est

commandé par le signal numérique crypté de réponse (I6) du dispositif d'identification.

- 8. Système selon l'une des revendications 1 à 7, **caractérisé par I fait que** le dispositif d'identification comporte une unité de décision de bits (115) dont la cadence de référence ($f'k$) est délivrée par la première boucle de verrouillage de phase (109), ladite unité de décision de bits recevant en entrée le signal d'interrogation, pour délivrer en sortie un signal numérique à ladite cadence de référence, représentant ledit signal d'interrogation. 5
- 9. Système selon l'une des revendications 1 à 8, **caractérisé par le fait que** le signal (V10) délivré en sortie par l'unité de décision de bits (67) de l'unité centrale est comparé par cette dernière avec un signal numérique crypté correspondant (g) engendré par l'unité centrale, afin d'authentifier le dispositif d'identification (I). 10 15 20
- 10. Système selon l'une des revendications 1 à 9, **caractérisé par le fait que** l'unité centrale comporte un oscillateur générateur d'onde porteuse en radiofréquence (55), relié à un modulateur de phase ou d'amplitude (56), qui est commandé par ledit signal numérique d'interrogation (V7) engendré par l'unité centrale. 25
- 11. Système selon la revendication 10, **caractérisé par le fait que** l'unité centrale est apte à commander successivement l'arrêt puis le démarrage de l'oscillateur (55) de l'unité centrale, selon que celle-ci est en phase d'émission du signal d'interrogation (V7), puis en phase de réception du signal de réponse. 30 35

40

45

50

55

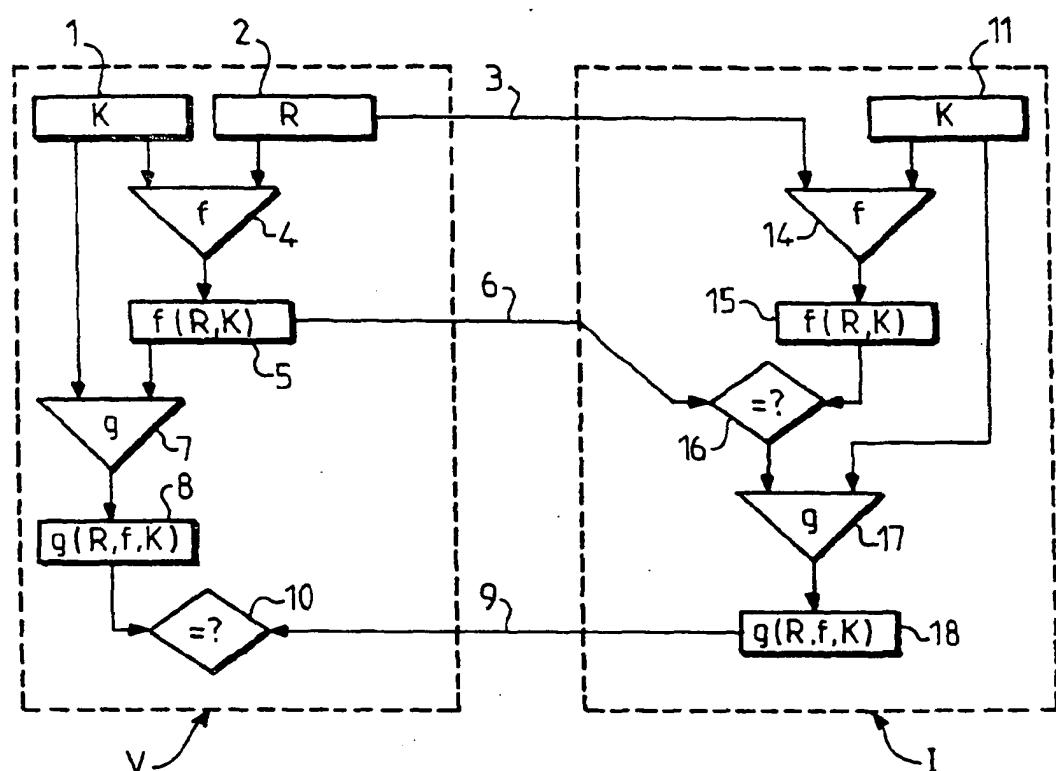


FIG. 1

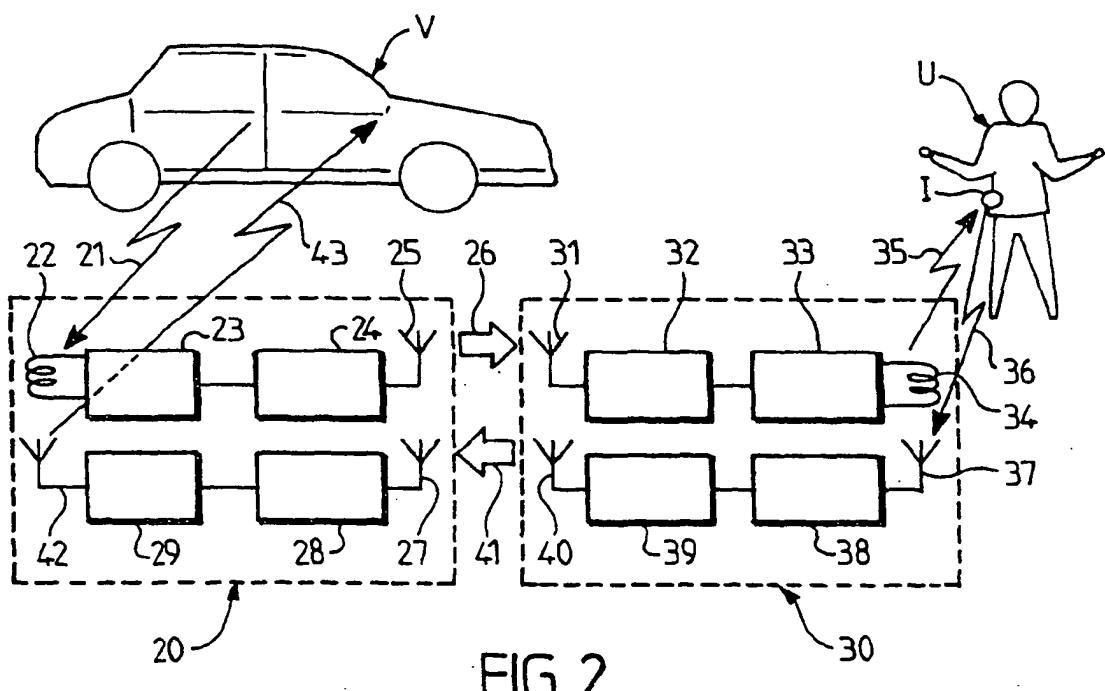


FIG. 2

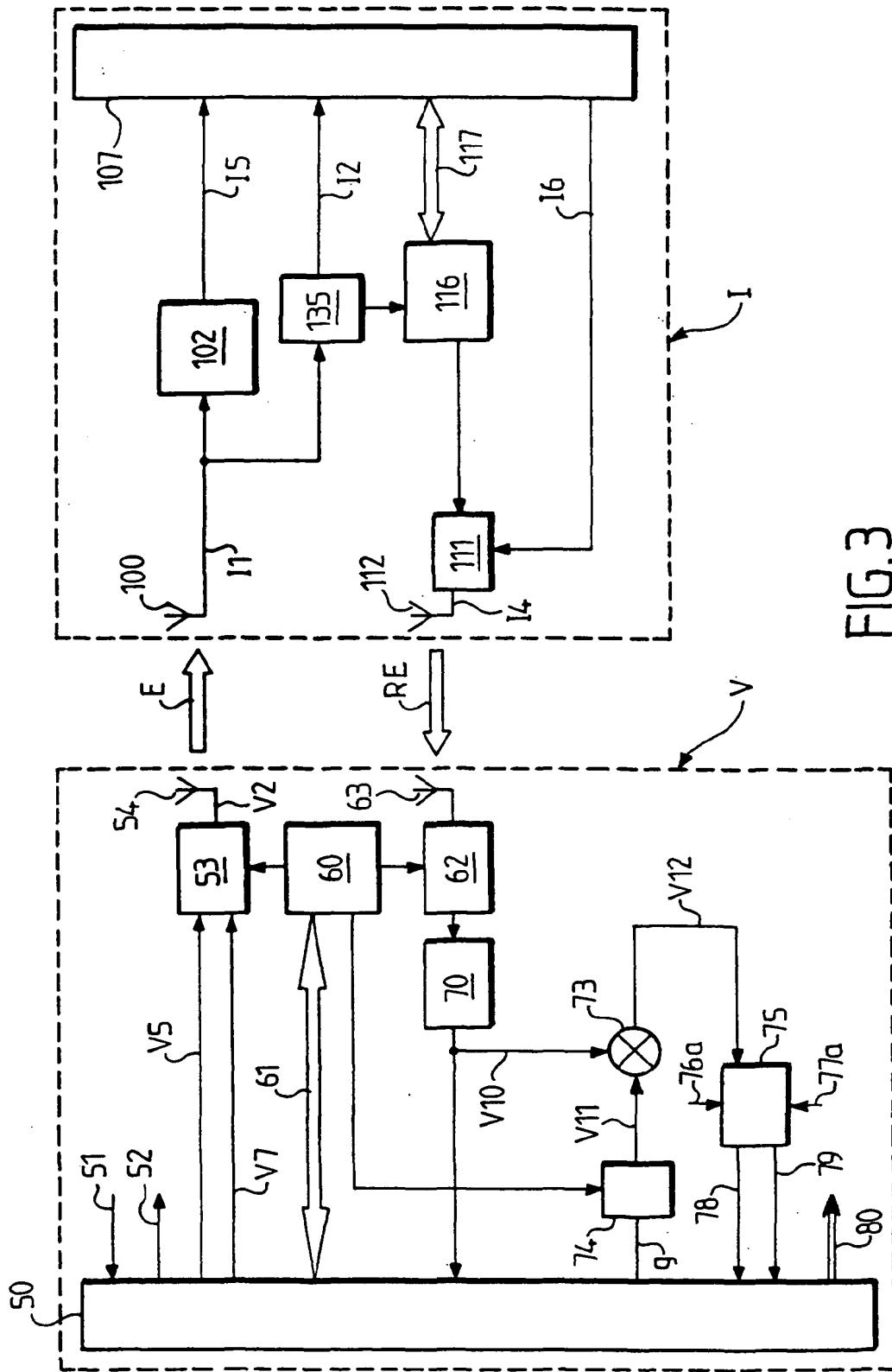


FIG. 3

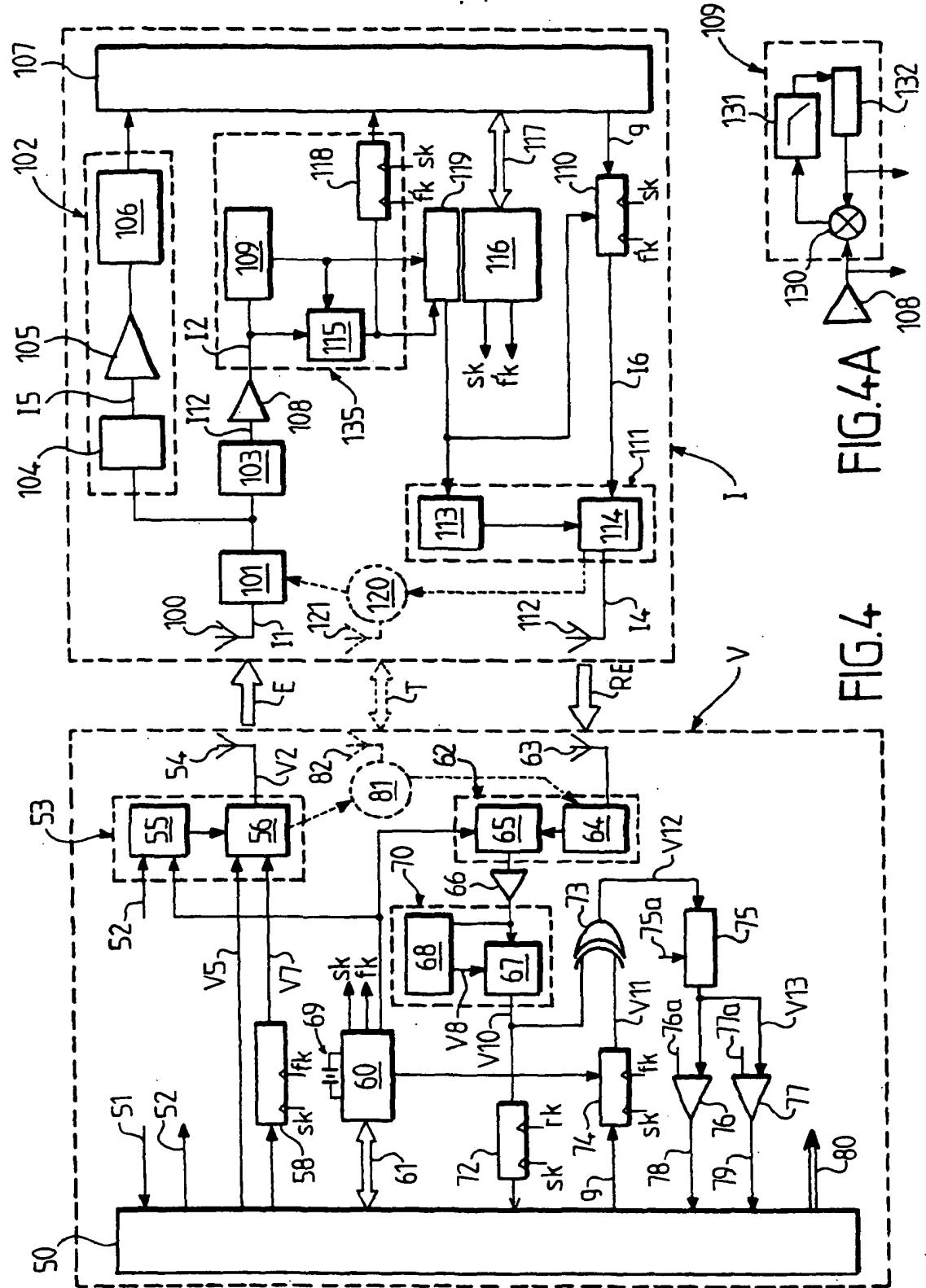


FIG. 4

FIG. 4A

FIG.5

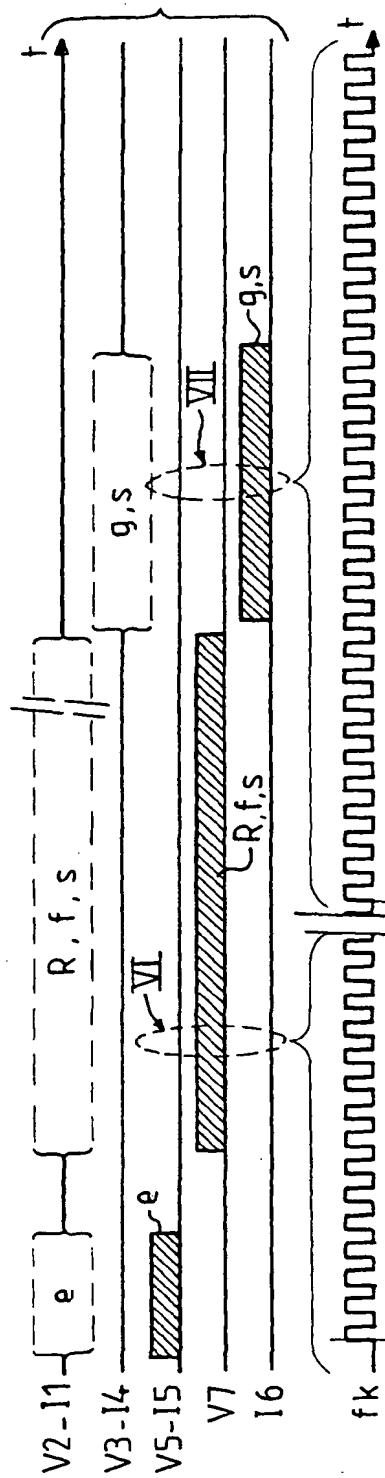
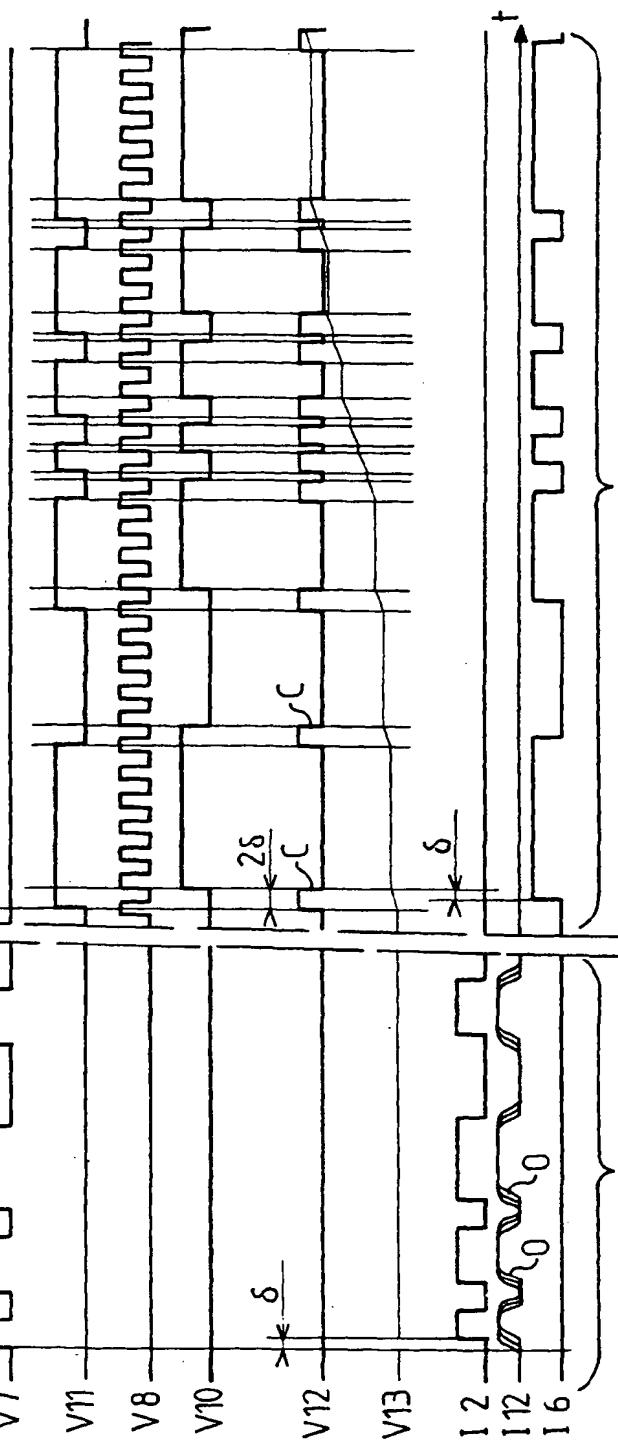


FIG.7

FIG.6





(19) Europäisches Patentamt
Europäischer Patent Office
Office européen des brevets



(11) EP 1 152 109 A3

(12)

DEMANDE DE BREVET EUROPEEN

(88) Date de publication A3:
05.12.2001 Bulletin 2001/49

(51) Int Cl.7: E05B 49/00, G01S 13/76

(43) Date de publication A2:
07.11.2001 Bulletin 2001/45

(21) Numéro de dépôt: 01401096.1

(22) Date de dépôt: 27.04.2001

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR

Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: 03.05.2000 FR 0005629

(71) Demandeur: Delphi Technologies, Inc.
Troy, MI 48007 (US)

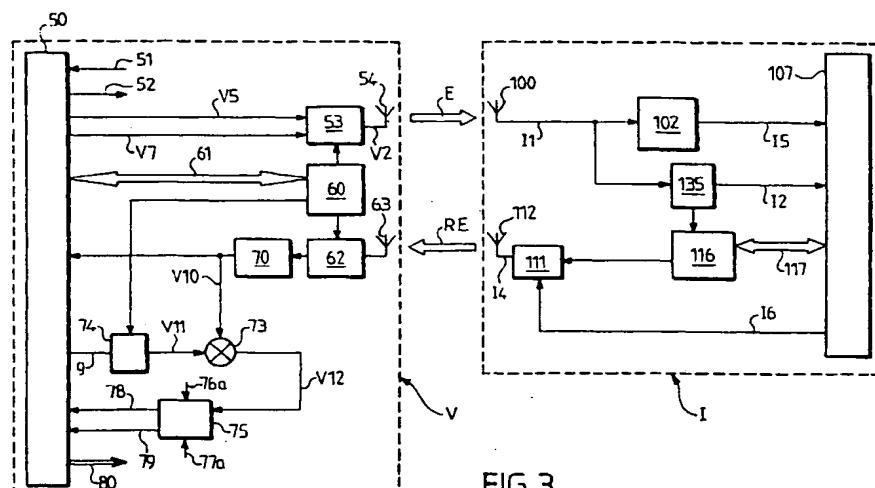
(72) Inventeur: Lelandais, Guy
91190 Gif-sur-Yvette (FR)

(74) Mandataire: Abello, Michel
Cabinet Peusset,
78, avenue Raymond Poincaré
75116 Paris (FR)

(54) Système pour le démarrage et/ou l'accès mains libres d'un véhicule automobile

(57) Système d'accès dit mains libres pour véhicule automobile (V), comportant une unité centrale apte à engendrer, à une cadence d'horloge haute prédéterminée un signal numérique représentatif de données d'authentification émis sous la forme d'un signal d'interrogation radio-fréquence, et destiné à être reçu par un dispositif d'identification (I), qui comporte une première boucle à verrouillage de phase (135) pour délivrer un signal d'horloge de référence dont la cadence est synchronisée avec celle du signal d'interrogation précédent, le dispositif d'identification étant apte à émettre un signal

crypté de réponse (16) en radio-fréquence vers l'unité centrale, et l'unité centrale comportant une deuxième boucle à verrouillage de phase (70) pour délivrer à une unité de décision de bits un signal d'horloge de référence dont la cadence est synchronisée avec celle du signal crypté de réponse, l'unité centrale comportant, en outre, un moyen pour déterminer le décalage temporel entre ledit signal (V10) délivré par l'unité de décision de bits et un signal crypté correspondant (V11) engendré par l'unité centrale à ladite haute cadence prédéterminée.





Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 01 40 1096

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
A	EP 0 676 650 A (DAIMLER BENZ AEROSPACE AG) 11 octobre 1995 (1995-10-11) * le document en entier * ---	1,7-10	E05B49/00 G01S13/76
A	EP 0 983 916 A (MARQUARDT GMBH) 8 mars 2000 (2000-03-08) * abrégé; figures 1-7 * * alinéa '0014! - alinéa '0021! *	1,7-10	
A	WO 00 12848 A (KOSTAL LEOPOLD GMBH & CO KG ;FROMM MICHAEL (DE); KRAMER DETLEV (DE)) 9 mars 2000 (2000-03-09) * abrégé; figures 6-8 * * page 18, ligne 35 - page 21, ligne 29 * -----	1,7-10	
DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)			
			E05B G01S B60R
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche	Date d'achèvement de la recherche	Examinateur	
LA HAYE	11 octobre 2001	Buron, E	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinent à lui seul	T : théorie ou principe à la base de l'invention		
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie	E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date		
A : amère-plan technologique	D : cité dans la demande		
O : divulgation non écrite	L : cité pour d'autres raisons		
P : document intercalaire	& : membre de la même famille, document correspondant		

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 01 40 1096

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne vise ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

11-10-2001

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)	Date de publication
EP 0676650	A	11-10-1995	DE EP	4421349 A1 0676650 A2	12-10-1995 11-10-1995
EP 0983916	A	08-03-2000	DE EP	19941428 A1 0983916 A1	15-06-2000 08-03-2000
WO 0012848	A	09-03-2000	DE DE DE AU WO EP	19839696 A1 19839695 C1 19926234 A1 5737299 A 0012848 A1 1109981 A1	02-03-2000 04-05-2000 14-12-2000 21-03-2000 09-03-2000 27-06-2001

EPO FORM P104/00

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No. 12/82

